UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

VICTORIA THOMAS, on behalf of herself and all others similarly situated, Plaintiff, v. APRIA HEALTHCARE, LLC, Defendant.	Case No.: 1:23-cv-1096 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Victoria Thomas ("Plaintiff") brings this Class Action Complaint on behalf of herself and all others similarly situated, against Defendant, APRIA HEALTHCARE, LLC ("Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Healthcare providers that handle sensitive, personally identifying information ("PII") and protected health information ("PHI") owe a duty to the individuals to whom that data relates, including patients and employees. This duty arises based upon the parties' relationship and because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data breach manifests in several ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that

risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take several additional prophylactic measures.

3. As a healthcare provider, Defendant is required by law to provide every patient with a Notice of Privacy Practices.

4. Defendant knowingly obtains patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

5. Plaintiff brings this class action on behalf of individuals, employees and patients of Defendant, or otherwise people that are customers of or have their records collected by Defendant, whose PII and/or PHI was accessed and exposed to unauthorized third parties during a data breach that was first announced by Defendant in May of 2023 (the "Data Breach").

6. From April 5, 2019 to May 7, 2019 and again from August 27, 2021 to October 10, 2021, the bad actor(s) had access to Defendant's network. Further, as part of the Data Breach, it is believed and averred that the bad actor(s) exfiltrated Plaintiff's and the class members' PII and PHI from Defendant's network.

7. Despite that Defendant became aware of the Data Breach on September 1, 2021, it failed to notify the Plaintiff and the putative Class Members until June 2023.

8. Plaintiff, on behalf of herself and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of fiduciary duty/confidence, breach of implied contract, unjust enrichment, and declaratory judgment, seeking actual and punitive damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

9. Based on the public statements of Defendant to date, a wide variety of PII and PHI was implicated in the breach. For patients, that includes: Social Security number, personal, medical, health insurance information, and financial information.

10. As a direct and proximate result of Defendant's inadequate data security, its breach of its duty to handle PII and PHI with reasonable care, and its failure to maintain the confidentiality of patients' medical records and PHI, Plaintiff's and Class Members' PII and/or PHI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

11. Plaintiff and Class Members are now at a significantly increased risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy protecting themselves, to the extent possible, from these crimes.

12. To recover from Defendant for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, along with declaratory judgment and injunctive relief requiring Defendant to, at minimum: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

13. Plaintiff Victoria Thomas is an adult individual who at all relevant times has been a citizen and resident of the State of Colorado. Plaintiff's PHI and PII records were maintained within Defendant's networks, as Plaintiff received medical equipment healthcare services from

Defendant for over ten years. Shortly after June 6, 2023, Plaintiff received a notice letter from Defendant informing Plaintiff that her PII and PHI may have been accessed or exposed to unknown, unauthorized third parties during the Data Breach, including but not limited to her name, email address, patient account number, patient dates of service, and device descriptions. Since that time, she has had identity-related issues with multiple accounts, including her Spotify and T-Mobile accounts, that, upon information and belief, occurred as a result of the Data Breach at issue here.

14. Defendant APRIA HEALTHCARE, LLC ("Defendant") is a Delaware limited liability corporation with its principal place of business at 7353 Company Drive, Indianapolis, Indiana 46237. Defendant is a provider of home healthcare equipment serving more than 2 million patients in the United States.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over this nationwide class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendant. See 28 U.S.C. § 1332(d)(2)(A). The Court has personal jurisdiction over Defendant because it owns and operates businesses that are located and headquartered in Indiana and conducts substantial business throughout Indiana.

16. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because a substantial part of the acts giving rise to Plaintiff's claims occurred in this district.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims

17. At all relevant times, Defendant knew it was storing and permitting its employees to use its internal network server to transmit valuable, sensitive PII and PHI and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

18. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

19. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

20. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[1] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

21. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the Identity Theft Resource Center ("ITRC"),

[1] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[2]

22. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[3]

23. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[4]

24. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[5]

25. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

26. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit

---

[2] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.

[3] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).

[4] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.

[5] *Id.*

cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[6] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[7]

27. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[8]

---

[6] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[7] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com /gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[8] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

28. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can **sell for up to $1,000 online.**"[9]

29. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[10]

30. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

B. Defendant Breached its Duty to Protect its PII and PHI

31. On September 1, 2021, Apria discovered that it had experienced a data breach relating to its internal systems.

32. According to Defendant, it conducted an investigation and determined that an unauthorized actor may have accessed sensitive information.

[9] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[10] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

33. All in all, more than 1.8 million individuals may have had their PII and/or PHI breached.

34. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its patients' PII and PHI.

35. Plaintiff received the notice from Defendant dated June 6, 2023, advising that Plaintiff was a victim of Defendant's data security failures exposing PHI and PII. The Notice is attached as Exhibit A.

36. Like Plaintiff, the Class Members received similar notices informing them that their PII and/or PHI was exposed in the Data Breach.

37. In its notice to Plaintiff and Class members, Defendant asserted: "[w]e take the protection and proper use of your information very seriously."

38. The notice letters were deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, when Defendant completed its investigation, why sensitive information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether Defendant knows if the data has not been further disseminated.

39. Defendant acknowledges that it is responsible to safeguard Plaintiff and Class Members' PHI and PII. It pledges that it takes privacy very seriously and makes numerous promises that it will maintain the security and privacy of PHI and PII.

40. Patients who receive healthcare services, such as Plaintiff, entrusted their PHI and PII to Defendant with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

41. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' PHI and PII from disclosure.

42. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they rely on Apria to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

43. Defendant was well aware that the PHI and PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes. As the Federal Trade Commission (FTC) recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and fraud.[11] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

44. The ramifications of Defendant's failure to keep PHI and PII secure are long lasting and severe. Once stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

45. Further, criminals often trade stolen PHI and PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PHI and PII on the internet, thereby making such information publicly available.

[11] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited June 2, 2023).

46. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[12] This time lag between when harm occurs versus when it is discovered, and also between when PHI and PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

47. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

48. Further, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

49. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the

[12] *Identity Theft and Your Social Security Number*, Social Security Administrative, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed June 2, 2023).

new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

50. Defendant knew, or should have known, the importance of safeguarding PHI and PII entrusted to it and of the foreseeable consequences if its systems were breached. This includes the significant costs that would be imposed on individuals as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

51. Plaintiff and Class Members now face years of constant surveillance of their records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PHI and/or PII.

52. Despite all of the publicly available knowledge of the continued compromises of PHI and PII, Apria's approach to maintaining the privacy of the PHI and PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

53. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be spared having to deal with the consequences of Defendant's misfeasance.

54. Once PHI and PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

55. The delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Plaintiff was not timely notified of the Data Breach, depriving her and the Class of the ability to promptly mitigate potential adverse resulting consequences.

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited June 2, 2023).

56. As a result of Apria's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. Actual identity theft;

b. Unauthorized use and misuse of their PII;

c. The loss of the opportunity to control how their PII is used;

d. The diminution in value of their PII;

e. The compromise, publication, and/or theft of their PII;

f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

h. Costs associated with placing freezes on credit reports;

i. Delay in receipt of tax refund monies or lost opportunity and benefits of electronically filing of income tax returns;

j. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

k. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as it fails to undertake appropriate measures to protect the PII in its possession; and

l. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

57. To date, Apria has not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, it has taken to secure the PHI and PII still in its possession. Through this litigation, Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses any harms, and ensure Defendant has proper measures in place to prevent another breach from occurring in the future.

58. Apria was expressly prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

59. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

60. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[15] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate

[14] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed June 2, 2023).

[15] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 2, 2023).

measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. Defendant failed to properly implement basic data security practices. Its failure to employ reasonable and appropriate measures to protect against unauthorized access to PHI and PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

63. Apria was at all times fully aware of its obligation to protect PHI and PII and was also aware of the significant repercussions that would result from its failure to do so.

C. Plaintiff and Class Members Suffered Damages

64. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

65. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

66. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

67. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[16]

68. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[17]

69. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[18]

70. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."[19]

71. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[20]

72. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft.

---

[16] https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

[17] https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.

[18] *Id.*

[19] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[20] *Id.*

Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[21]

73. Plaintiff and the Class members have also been injured by Defendant's unauthorized disclosure of their confidential and private medical records and PHI.

74. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

CLASS ALLEGATIONS

75. Plaintiff bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following classes:

> **Nationwide Class**
> All individuals in the United States whose PII and/or PHI was maintained by the Defendant and who were sent a notice of the Data Breach.
>
> **Colorado Sub Class**
> All individuals in Colorado whose PII and/or PHI was maintained by the Defendant and who were sent a notice of the Data Breach.

76. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

77. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

---

[21] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

78. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. Based on public information, the Class includes over 1.8 million individuals.

79. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had a duty to maintain the confidentiality of Plaintiff and Class Members' PHI;

c. Whether Defendant breached its obligation to maintain Plaintiff and the Class members' medical information in confidence;

d. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

e. Whether Defendant breached its fiduciary duty to Plaintiff and the Class.

f. Whether Defendant failed to properly give notice;

g. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

h. Whether Plaintiff and Class Members are entitled to restitution or disgorgement as a result of Defendant's wrongful conduct; and

i. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

80. **Typicality**. Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII and PHI. Plaintiff and Class Members all entrusted their PII and PHI to Defendant, and each of them had their PII and PHI obtained by an unauthorized third party.

81. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because their interests do not conflict with the interests of the other Class Members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

82. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its common law and statutory duties to secure PII and PHI on its network server, then Plaintiff and each Class Member suffered damages from the exposure of their sensitive personal information in the Data Breach.

83. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

84. **Manageability.** While the precise size of the Class is unknown without the disclosure of Defendants' records, public records indicate at least 1.8 million individuals whose PII and/or PHI was compromised in the Data Breach. The claims of Plaintiff and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE and NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Classes)

85. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

86. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

87. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

88. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

89. Defendant's duty also arose from Defendant's position as a provider of healthcare. Defendant holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Defendant, as a direct healthcare provider, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

90. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices published to its patients.

91. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

92. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

93. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of a data breach involving PII and PHI of its patients.

94. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

95. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

96. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act was intended to guard against.

97. Pursuant to Defendant's May 2, 2022 Notice of Privacy Practices, it acknowledged its legal duties by stating that it was "required by law to maintain the privacy of your protected health information ("PHI"), to provide you with this Notice of our legal duties and privacy practices with respect to your PHI, and to notify you if a breach of your PHI occurs, in accordance with applicable law." *See* https://www.apria.com/hubfs/GEN-4539_Form_Notice-Privacy-Practices_04-22_v2_FNL.pdf (last accessed June 21, 2023).

98. Defendant violated its own policies by actively disclosing Plaintiff's and the Class Members' PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI; failing to maintain the confidentiality of Plaintiff's and the Class Members' records; and by failing to provide timely notice of the breach of PHI to Plaintiff and the Class.

99. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Loss of their privacy and confidentiality in their PHI;

j. The erosion of the essential and confidential relationship between Defendant – as a health care services provider – and Plaintiff and Class members as patients; and

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received.

100. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Classes)

101. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

102. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

103. As a healthcare provider, Defendant has a fiduciary relationship to its patients, like Plaintiff and the Class Members.

104. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable PII and PHI related to Plaintiff and the Class, which it was required to maintain in confidence.

105. Defendant owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and

protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

106. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiff and the Class members' medical records.

107. Patients like Plaintiff and Class members have a privacy interest in personal medical matters, and Defendant had a fiduciary duty not to disclose medical data concerning its patients.

108. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII and PHI of Plaintiff and Class members, information not generally known.

109. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their PHI to an unknown criminal actor.

110. Defendant breached the duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; and (h) making an

unauthorized and unjustified disclosure and release of Plaintiff and the Class members' PHI and medical records/information to a criminal third party.

111. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their privacy, confidences, PII, and PHI would not have been compromised.

112. As a direct and proximate result of Defendant's breach of its fiduciary duties and breach of its confidences, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Loss of their privacy and confidentiality in their PHI;

j. The erosion of the essential and confidential relationship between Defendant – as a health care services provider – and Plaintiff and Class members as patients; and

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendant.

113. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

114. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

115. When Plaintiff and members of the Class provided their personal information to Apria, Plaintiff and members of the Class entered into implied contracts with Apria pursuant to

which Apria agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

116. Defendant required Plaintiff and class members to provide and entrust their PHI and PII and financial information as a condition of obtaining Defendant's services.

117. Plaintiff and Class members would not have provided and entrusted their PHI and PII and financial information to Apria in the absence of the implied contract between them and Apria.

118. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Apria.

119. Apria breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the personal information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

120. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

121. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

122. This count is brought in the alternative to Plaintiff's breach of contract count. If claims for breach of contract are ultimately successful, this count will be dismissed.

123. Plaintiff and Class members conferred a benefit on Apria by way of customers' paying Apria to maintain Plaintiff and Class members' personal information.

124. The monies paid to Apria were supposed to be used by Apria, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class members.

125. Apria failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class members, and as a result Apria was overpaid.

126. Under principles of equity and good conscience, Apria should not be permitted to retain the money because Apria failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal information that they paid for but did not receive.

127. Apria wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class members.

128. Apria's enrichment at the expense of Plaintiff and Class members is and was unjust.

129. As a result of Apria's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Apria, plus attorneys' fees, costs, and interest thereon.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Classes)

130. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

131. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

132. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendant is currently maintaining data

security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate, contrary to Defendant's assertion that it has confirmed the security of its network. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and/or PHI will occur in the future.

133. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure PII and PHI and to timely notify employees, patients or any individuals impacted of a data breach under the common law, Section 5 of the FTC Act, HIPAA, various state statutes, and the common law; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PII and PHI.

134. This Court also should issue corresponding prospective injunctive relief requiring Defendant to, at minimum 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of Plaintiff and Class members' PII and PHI possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

135. If an injunction is not issued, Plaintiff and the Classes will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs,

Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

136. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

137. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, pray for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: June 23, 2023

Respectfully Submitted,

/s/ William N. Riley
William N. Riley (#14941-49)
Russell B. Cate (#27056-29)
Sundeep Singh (#26591-29)
RILEYCATE, LLC
11 Municipal Dr., Suite 320
Fishers, IN 46038
Tel: (317) 588-2866
Fax: (317) 458-1785
wriley@rileycate.com
rcate@rileycate.com
ssingh@rileycate.com

KENNETH J. GRUNFELD, ESQUIRE
KEVIN FAY, ESQUIRE
GOLOMB SPIRT GRUNFELD P.C.
1835 Market Street, Suite 2900
Philadelphia, Pennsylvania 19103
Telephone: (215) 346-7338
Facsimile: (215) 985-4169
KGrunfeld@GolombLegal.Com
Kfay@GolombLegal.Com